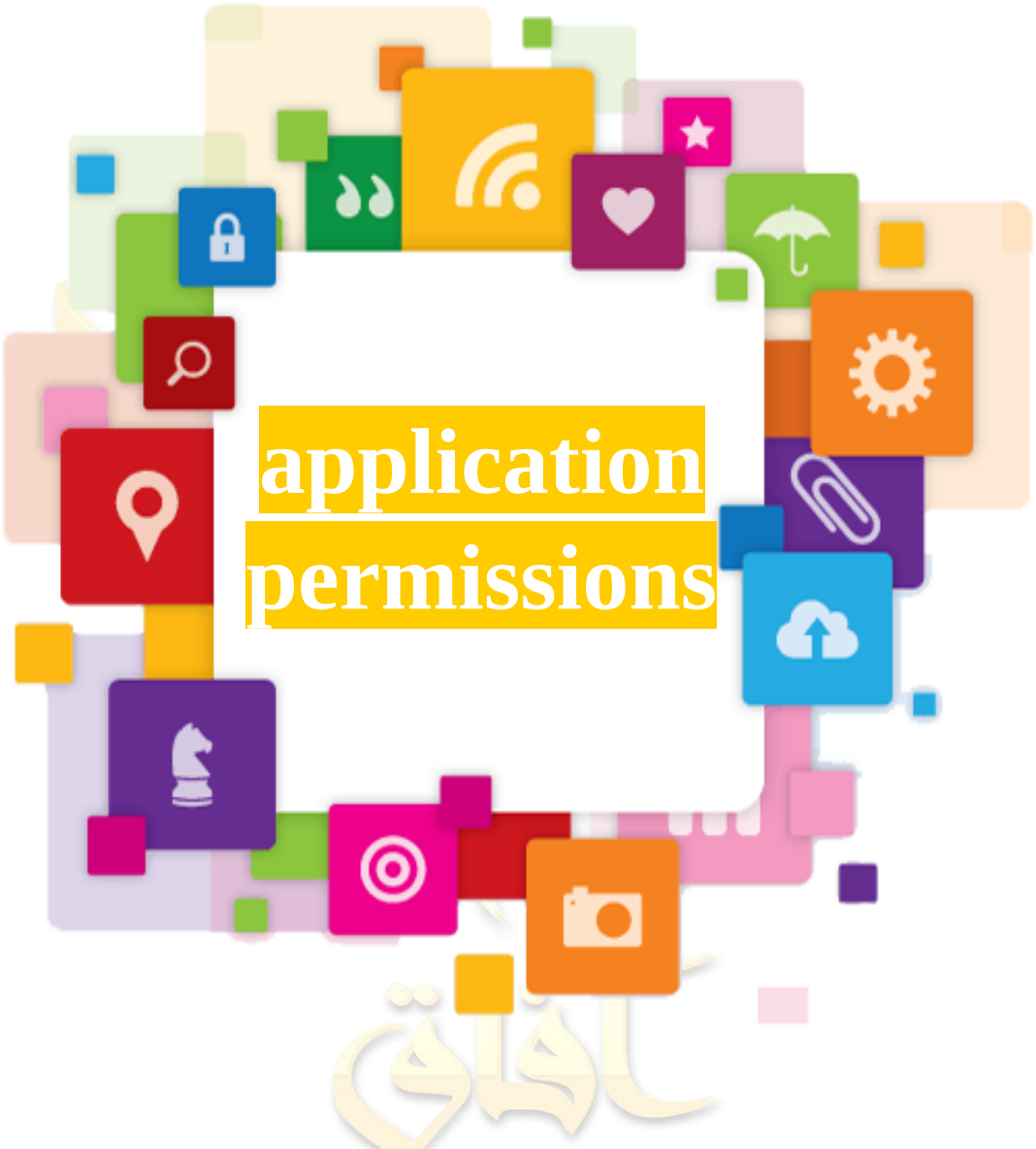


application permissions

Our phones today carry all our secrets and they do not leave us at all times unlike the personal computer or mobile, these phones carry our pictures and messages know who we call and when and know all the places we hesitate and the capabilities of our mobile phones increased as well as we have become miniature computers carrying dozens if not hundreds of Programs We download these programs often without knowing what these programs are doing. Or what powers do they require?

الحمدلله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام على من أعلى الله منار الاسلام بسيفه وعلى اله وصحبه ومن تبعهم باحسان الى يوم الدين اما بعد ..

First Lesson: From series the security of smartphones

application permissions

Our phones today carry all our secrets and they do not leave us at all times unlike the personal computer or mobile, these phones carry our pictures and messages know who we call and when and know all the places we hesitate and the capabilities of our mobile phones increased as well as we have become miniature computers carrying dozens if not hundreds of Programs We download these programs often without knowing what these programs are doing. Or what powers do they require?

Many applications violate the privacy of users where the synchronization of private messages, contacts, device metadata, images, files and other sensitive data, so control the powers of applications is imperative to maintain your privacy and prevent the sharing of your personal information with unknown parties for propaganda or intelligence purposes

So .... How do we get rid of these powers and prevent applications from accessing them

Note

The first and second methods do not need technical skills to use them. Method 3, 4, and 5 require advanced technical skills to install the application control tools

| Method 1:application permissions |

In Android 6.0 versions there are 7.2 power management (application permissions) by default

- **Go to Settings and then Settings Manager**

- **Then select the application**

❍ **Click License**

- **These are the permissions and you will find all permissions enabled**

- **Cancel the activation of the validity that you want to prevent the application from accessing**

|Method2*:* APK PERMISSION REMOVER |

A simple and simple way to rely on reverse engineering of the application but not effective in all applications where you can not delete or ban powers that are essential and the application will stop if you delete them

❍ **Upload APK PERMISSION REMOVER PRO official version paid [here](#)**

| Paid version features

- The application does not contain advertisements
- Allows to modify the permissions of more than 10 applications
- The application's function is to modify the APK and permanently delete the application's permissions
- To select an APK on memory, press Open an apk
- To select a installed application, press Open an app

- You will see a list of the applications installed on your phone
- Select the application to edit or deauthorize

- These are the application's powers
- To delete the validity, press the ☑ sign next to the validity to become☒
- Then press SAVE & RE INSTALL


TextNow
PERMISSION
IMAGE
MANIFEST
device without showing them to you.
Camera
Take pictures and videos
android.permission.CAMERA
Allows the app to take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation.
Microphone
Record audio
android.permission.RECORD_AUDIO
Allows the app to record audio with the microphone. This permission allows the app to record audio at any time without your confirmation.
Your location
Approximate location (network-based)
android.permission.ACCESS_COARSE_LOCATION
Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.
Your social information
Read your contacts
android.permission.READ_CONTACTS
Save & Re-Install
Close


Working Hard ...
TECH_SUPPORT
SR444TAW

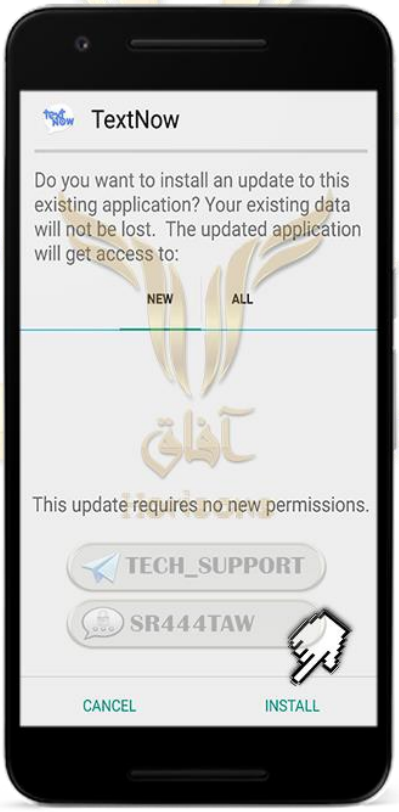
❍ **Now delete the old version of the application you have modified and install the new modified version**

❍ **Press unistall to delete the old version and after deletion press install to install the modified version**

Important

Before you modify the application, verify that it is transferring data to another application or device

❍ **Complete the steps of the app install**



Important

Easy way to work on all versions of Android from 3.2 to 0.6, depending on the reverse engineering of the application, but you can not control all the powers where there are basic powers depend on the application during the operation such as access to the Internet or read the internal memory if you delete the application will destroy but verify before installing Apps from deleting powers that violate your privacy such as syncing your phone history, reading phone status, and accessing location, camera, and mike

****

| Method 3:Feature. Privacy Guard |

Privacy Guard is a virtual feature with Lineage OS that allows the user to control the powers of general applications such as access to contacts and geographical location

❍ **Do the options shown in the following image to automatically activate the PrivacyGuard feature for newly installed applications**

❍ **Click Allowed to grant the application access to the permissions**

❍ **Click Ignored to prevent the application from accessing the permissions**

❍ **Click Always ASK to show a notification when the app reaches the validity of your location**

❍ **Click Advanced for advanced settings**

❍ **Through the following settings you can see which applications have access to your geographical location or messages**

❋❋❋❋❋❋❋❋❋❋

Important Notice: Support for Xposed Framework has been lifted due to security vulnerabilities that pose a threat to users' security. We do not recommend using Xposed applications

Xposed 【 Method 4: Xprivasy 】

An open-source Xprivasy application developed by a member of the XDA Developers site was awarded the Best Appraisal App for 2013 from BlackDuck

Xprivasy is one of the best applications that allows full control of the powers of applications installed on the machine, where it has many features to manage the powers of applications

Xprivasy does not delete permissions from the application, but it provides applications that want access to a certain validity as your location fake fake data or prohibit it from accessing this authority, unlike other applications such as Apk permission Remover or ADV Permission Remover. These applications are based on reverse engineering Application and applications often stop when you remove or delete their basic privileges

- **You must have a RUT permission if you do not know what routine or method to install it click here**

- **Take a backup of the system if you do not know the way to go to this link from here**

- **Install the Xposed Framework**

- **Download the Xprivasy application from Google Play Store or Xposed Installer**

❍ **Xprivacy application interface**

|| Application settings ||

Sort | Choose to browse applications based on name or date of installation

FILTER | To filter applications such as showing main system applications with installed applications or showing installed applications only

Usage Data | To review a list of permissions that applications have requested access to or have been rejected by Xprivasy


XPrivacy
Pro version
All
Check to restrict:
Sort
Filter
Usage data
Template
Operations ...
Switch theme
Settings
Help ...
10167 Amaze
10166 Android
10165 AnySoft
10164 AnySoft Language Pack
10163 APK Edi
10162 APK Permission Remover
10161 App Cloner
10160 App Manager
10159 Applications Info
10158 Brave
10157 Challegram


XPrivacy
301/5424 3.57/s
Long press function name to white or black list parameter
13:22:20 1000 internet/connect connectivitycheck.gstatic.com:80
13:22:20 1000 network/NetworkInfo.getExtraInfo
13:22:20 1000 internet/InetAddress.getAllByNameOnNet connectivitycheck.gstatic.com
13:22:17 10174 internet/ Connectivity.getActiveNetworkInfo
13:22:17 10174 internet/NetworkInfo.isConnected
13:22:17 10174 internet/NetworkInfo.getDetailedState
13:22:17 10174 internet/LinkProperties.getLinkAddresses
13:22:17 10174 phone/getSimOperator
13:22:17 10156 internet/NetworkInfo.isConnected
13:22:17 10156 internet/ Connectivity.getActiveNetworkInfo
13:22:17 10156 internet/NetworkInfo.getDetailedState
13:22:17 10156 internet/LinkProperties.getLinkAddresses
13:22:17 10174 accounts/getAccountsByTypeForPackage com.google
13:22:17 10174 phone/Configuration.MNC
13:22:17 10174 phone/Configuration.MCC
13:22:17 10075 ipc/Binder IPackageManager:getPackageUid
13:22:17 10074 ipc/Binder IPackageManager:getPackageUid
13:22:16 10097 internet/ Connectivity.getActiveNetworkInfo
13:22:16 10097 internet/NetworkInfo.isConnected
13:22:16 10097 internet/NetworkInfo.getDetailedState
13:22:16 10097 internet/LinkProperties.getLinkAddresses
13:22:16 10097 internet/NetworkInfo.getState
13:22:16 10097 internet/Connectivity.getNetworkInfo
13:22:15 10097 ipc/Binder IActivityManager:REF_CONTENT_PROVIDER
13:22:15 10097 ipc/Binder

Tamplate | To set default settings to block access from publicly installed applications, for example, you can block all newly installed applications from accessing your location

❍ **Activate the option next to the? To be activated ✓ that is, your installed applications have become blocked from accessing this authority that you have specified**

❍ **Then press Done**

Operations | Xprivacy Advanced Settings (available in paid version)

Select All | To select all applications installed on the device

Toggle restrictions | Toggle Block (Clear previous block settings)

Export | Save a file for Xprivacy settings on the system

Import | Adds a file to the Xprivacy settings on the system

Submit restrictions | To apply blocking and control privileges to all applications

Fetch restrictions | Displays the permissions for installed applications

Switch theme | To change the color of the theme


XPrivacy
Pro version
All
Check to restrict:
10167 Amaze
10166 Android
10165 AnySoft
10164 AnySoft Language Pack
10163 APK Edi
10162 APK Permission Remover
10161 App Cloner
10160 App Manager
10159 Applications Info
10158 Brave
10157 Challegram
Sort
Filter
Usage data
Template
Operations ...
Switch theme
Settings
Help ...

Settings |


XPrivacy
Pro version
All
Check to restrict:
10167 Amaze
10166 Android
10165 AnySoft
10164 AnySoft Language Pack
10163 APK Edi
10162 APK Permission Remover
10161 App Cloner
10160 App Manager
10159 Applications Info
10158 Brave
10157 Challegram
Sort
Filter
Usage data
Template
Operations ...
Switch theme
Settings
Help ...

- **Make sure you activate the first three options**

In the Settings box, you will find below other options:

- **Verify that the Randomize on boot option is enabled after the boot**

- **Then click randomize NOW Random**

- **Activating all the options below the MAC address, ID, phone ID, etc., where Xprivasy will provide applications with counterfeit data**

- **Then press the ١disk icon above to save the adjustments**

- **Return to the application interface**

- **The blue option indicates the box to close the application's permissions**

- **The default option indicates the activation of the question property when the application requests access to a specific validity as in the following image**

In the following example, the Xprivacy application displays a notice to block or allow the Protonmail application to gain access to the Internet

Category | Where the type of validity appears - in the following example Internet shows access to the Internet

Functions | The validity function appears - in the following example, the validity function is defined as the connection

parameters | The IP address and port to be accessed by the application appear

Expert mode |Advanced settings to control the validity of a particular application where you can give the application access to the Internet for only 15 seconds by activating the option for once for 15 S and then the notification appears again after 15 seconds, and the option to apply to Category

Category | is to block / On the Internet either the option of Whit / Blacklist to insert the IP address and port to the Automatic Block List or Blacklist Allow Whitelist

- **Select any application to modify its powers**

؟To activate the question property when the application requests access to a specific validity

✓ Close the application's validity

To show more control options

Important

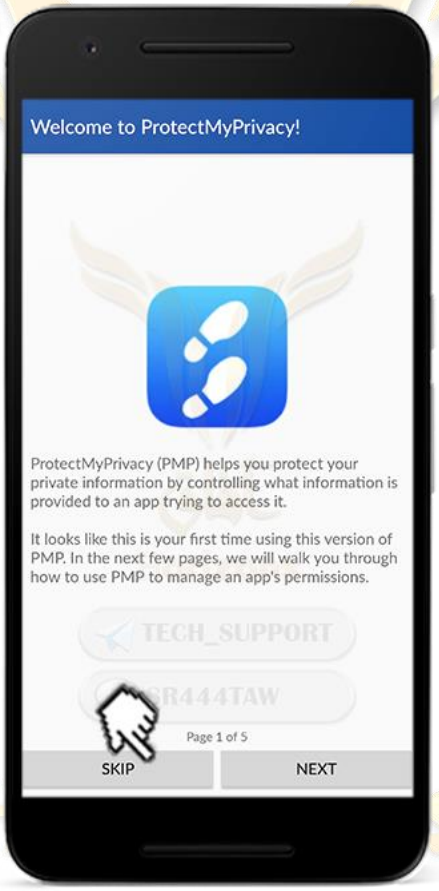
Some applications may be disabled when they are denied access to basic privileges so be careful while using Xprivasy You can use applications that give you an unlimited trial period by preventing these applications from accessing your phone data such as your IP address, MAC address, IMEI number,

****

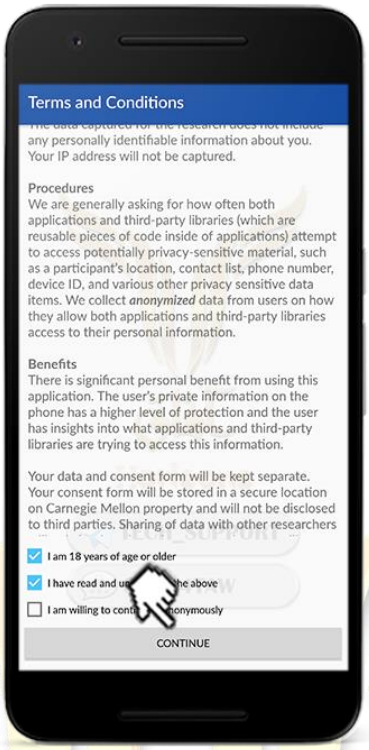
XPOSED 【Method 5: Protect My Privacy (PMP) 】

Allows the user to protect personal data on Android devices, which provides an additional layer of protection between applications and operating system, which gives the user the ability to control the authority of applications installed on the device and by providing applications with false data or prevent arbitrary access to certain powers

- **Go to the Xposed installer and look for the Protect My Privacy (PMP) application and make sure that the latest version**
- **Click Skip**



- **Press CONTINUE**



Protected Apps| All applications are protected by PMP implementation

System Apps| System applications

Third party|Third-party application libraries that violate your privacy

❍ **Select the application**

❍ **After choosing the application you can control the permissions either Deny Deny or allow Allow or send false data to the application Fake**

❍ **You can also click Reset App Permission To Ask to display a notifications window with the previous options to control the application permissions when running it, such as the following application**

❍ **Return to the interface and direct to the settings by pressing Settings**

Firewall Settings| Firewall settings

Choose fake location| To choose a fake geographic location

- **Firewall settings allow you to block IPv6 connection, since most VPN services leak IP address to IPv6 except some services such as F-Secure Freedome or NordVPN**

Reset Permissions| Reset to default settings

Set Default Permission Groups Behavior| To set the app permissions in general

Choose fake location| To choose a fake geographic location

Important

Use the PMP application with Xprivasy to prevent your personal data from being leaked to applications and not to be used as an alternative to Xprivasy

****

لاتنسونا من دعائكم


آفاق
Horizons